

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with
"KATINAGENEVA@GMAIL.COM" that is stored at
premises controlled by Google

Case No. 1:21MJ

387

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1957	Money Laundering - Transactions
15 U.S.C. § 645	False Statements to the SBA

The application is based on these facts:

See affidavit of Special Agent Steven Robinson.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

1/s/ Steven Robinson

Applicant's signature

Special Agent Steven Robinson

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone after e-mailly doubts (specify reliable electronic means).

Date:

10/05/21

City and state: Greensboro, North Carolina

L. Patrick Auld

Judge's signature

Honorable L. Patrick Auld

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Google account “KATINAGENEVA@GMAIL.COM” that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (“Google”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 17, 2021, with the Google Reference Number 6692298, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from April 1, 2020 to September 30, 2020, unless otherwise indicated:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 1343 (Wire Fraud), and 1957 (Monetary Transactions) and Title 15, United States Code, Section 645(a) (False Statement on Small Business Loan Application) involving Katina Graham, those violations occurring between on or about April 1, 2020 through September 30, 2020, namely:

- a. Records and information referencing the Economic Injury Disaster Loan program (“EIDL”);
- b. Records and information referencing Meuth Farms;
- c. Records and information referencing Katina Graham LLC;
- d. Documents or communications between and among Graham and any individuals regarding the receipt, funding, use, and transfer of EIDL proceeds; and
- e. Evidence indicating how, when, and by whom, the SUBJECT ACCOUNT was accessed and used for any of the items authorized for seizure by the warrant, including records that help reveal the whereabouts of such person(s).

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
GOOGLE ACCOUNT
“KATINAGENEVA@GMAIL.COM” THAT
IS STORED AT PREMISES CONTROLLED
BY GOOGLE LLC

Case No. 1:21mj387

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Steven Robinson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses. I am a Special Agent (SA) with the United States Secret Service (USSS). I have been employed with the USSS as a Special Agent since February 19, 2019. I have completed extensive training at both the Criminal Investigator Training Program at the Federal Law Enforcement Training Center, Glynco, Georgia and the Special Agent Training Course at the USSS training facility located in Beltsville, Maryland. During my time with the USSS, I have completed over 400 hours of training in cyber and computer-related investigations. Prior to my employment with the USSS, I was a Special Agent with the Diplomatic Security Service of the United States Department of State for three years.

2. I make this affidavit in support of an application for a search warrant for information associated with Google Account—katinageneva@gmail.com—the “SUBJECT ACCOUNT”) that is stored at premises owned, maintained, controlled, or operated by Google

LLC (“Google”), an electronic communications service provider, headquartered at 1600 Amphitheater Parkway, Mountain View, California.

3. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

4. Based on the facts as set forth in this affidavit, I submit that there is probable cause to believe that Katina Geneva Graham (“GRAHAM”), user of the SUBJECT ACCOUNT, committed violations of Title 18, United States Code, Section 1343 (wire fraud) and Title 18, United States Code, Section 1957 (engaging in monetary transactions in property derived from specific unlawful activity), as well as Title 15, United States Code, Section 645(a) (false statement on a small business loan application) (collectively, the “SUBJECT OFFENSES”). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes as further described in Attachment B.

5. This affidavit is based on my personal investigation and investigation by others. The facts contained herein have been obtained by interviewing witnesses and examining documents obtained in the course of the investigation, as well as through other means. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Background on CARES Act Relief

7. The Coronavirus Aid, Relief, and Economic Security (“CARES”) Act is a federal law enacted in or around March 2020 and designed to provide emergency financial assistance to the millions of Americans who are suffering negative economic effects caused by the COVID-19 pandemic. One source of relief provided by the CARES Act was the authorization of loans to small businesses for job retention and certain other expenses, authorizing up to \$349 billion in forgivable loans through a program referred to as the Paycheck Protection Program (“PPP”). In or around April 2020, Congress authorized over \$300 billion in additional PPP funding.

8. The Economic Injury Disaster Loan (“EIDL”) program is a Small Business Association (“SBA”) program that provides low-interest financing to small businesses, renters, and homeowners in regions affected by declared disasters.

9. The CARES Act also authorized the SBA to provide EIDLs of up to \$2 million to eligible small businesses experiencing substantial financial disruptions due to the COVID-19 pandemic. In addition, the CARES Act authorized the SBA to issue advances of up to \$10,000 to small businesses within three days of applying for an EIDL. The amount of the advance was

determined by the number of employees the applicant certifies having. The advances do not have to be repaid.

10. In order to obtain an EIDL and advance, a qualifying business must submit an application to the SBA and provide information about its operations, such as the number of employees, gross revenues for the 12-month period preceding the disaster, and cost of goods sold in the 12-month period preceding the disaster. In the case of EIDLs for COVID-19 relief, the 12-month period was that preceding January 31, 2020. The applicant must also certify that all of the information in the application is true and correct to the best of the applicant's knowledge.

11. EIDL applications are submitted directly to the SBA and processed by the agency with support from a government contractor, Rapid Finance. The amount of the loan, if the application is approved, is determined based, in part, on the information provided by the application about employment, revenue, and cost of goods, as described above. Any funds issued under an EIDL or advance are issued directly by the SBA. EIDL funds can be used for payroll expenses, sick leave, production costs, and business obligations, such as debts, rent, and mortgage payments. If the applicant also obtains a loan under the PPP, the EIDL funds cannot be used for the same purpose as the PPP funds.

Fraudulent Loan Applications: Background

12. The affiant knows from training and experience, and consultations with other federal agents, that since the time CARES Act relief became available, some individuals fraudulently sought such relief funds through a variety of means including, but not limited to: (1) applying for EIDL advances and loans on behalf of ineligible newly-created, shell, or non-existent businesses, and diverting the funds for illegal purposes; (2) submitting identical loan applications and supporting documents under the names of different companies; and (3) fraudulently obtaining

and using identifying information associated with individuals and/or businesses, applying for a loan using that information without the knowledge of those individuals and/or businesses, and diverting the funds to an unlawful recipient.

13. As described in further detail below, there is probable cause to believe that GRAHAM engaged in a scheme to fraudulently obtain COVID-19 relief funds through the use of stolen identities and nonqualifying businesses. GRAHAM, a resident of Durham, North Carolina, received payments from the EIDL program totaling \$151,600 from two separate EIDL applications that were submitted and approved for funding. The first EIDL application (the “Meuth Farms application”) raised suspicion because, as further described below, it sought funding for a business located in Texas and was submitted using the identifying information of an individual named C.M. However, the loan proceeds were deposited into a Wells Fargo bank account opened by Graham on June 26, 2020—days before the loan was disbursed. The second EIDL application (the “Katina Graham LLC” application) raised suspicion because the funds were sent to GRAHAM’s personal checking account at Carolinas Telco Federal Credit Union (CTFCU) and because of Graham’s link to the Meuth Farms application.

The Meuth Farms EIDL Application & Loan

14. On or about June 20, 2020, an online application for an EIDL was submitted from an IP address in Texas. The application listed the business name as “Meuth Farms” and the owner of the business as an individual with the initials, “C.M.” “Meuth Farms” was described as a sole proprietorship located in Houston, TX. The company was described as an agricultural business with 29 employees that has been in business since July 4, 2010.

15. Research conducted as part of this investigation, using public records and state business registration databases, found only one registered company named “Meuth Farms” in the

United States, but it is located in Illinois and does not appear to have any connection to C.M. or the purported Meuth Farms in the EIDL application. Further research showed that the personal information provided for C.M. in the application appears to be legitimate, including her home address, date of birth, and social security number (“SSN”). SBA records show that on October 1, 2020, an individual called the SBA, referenced this EIDL information, and stated that she had received a loan statement but had not applied for the loan and did not own a small business. This caller is believed to be C.M. based on the fact that the loan statement would have been sent to C.M.’s home address, which was listed on the EIDL application as the primary address for the applicant. However, the SBA was not able to confirm the caller’s identity.

16. The “business address” listed on the EIDL application, which also appeared to be a previous address for C.M., is a residence in an urban area of Houston with no apparent agricultural function.

17. The EIDL agreement was signed electronically by a person purporting to be C.M. on June 21, 2020.

18. On June 30, 2020, \$96,500 in EIDL funds were deposited into a bank account in GRAHAM’s name at Wells Fargo. On July 7, 2020, an advance of \$10,000 associated with the loan was deposited into the same account.

19. Bank records and other supporting documentation were received from Wells Fargo during the course of the investigation. Those records reveal that GRAHAM opened this account on June 26, 2020 (four days prior to the EIDL fund deposit). GRAHAM’s name, date of birth, address, and driver’s license number are listed on the account opening document. However, the SSN listed on the bank account application is not GRAHAM’s true SSN. The e-mail address listed on the application is “thekatinagraham@gmail.com.”

20. Bank records show that \$36,000 was withdrawn from the account shortly after the loan deposit—\$18,000 in cash was withdrawn between June 30, 2020 and July 1, 2020, and two cashier's checks for \$9,000 each were issued on July 1, 2020. The cashier's checks were made payable to Andrea Smith. GRAHAM stated in an interview, on April 26, 2021, that these funds were intended for a new business that she and Smith were starting, which is not a legitimate use of EIDL funds according to the contract that each applicant signs. This account was closed by Wells Fargo on September 17, 2020 due to suspected fraud. GRAHAM was issued a check for the remaining balance of \$69,980, which GRAHAM cashed at a check cashing business in Durham, NC on October 26, 2020. Records received from the check cashing business show an individual who appears to be GRAHAM on the surveillance camera cashing the check. GRAHAM also admitted to cashing this check in an interview on April 26, 2021.

The "Katina Graham LLC" EIDL Application & Loan

21. On June 23, 2020, an EIDL application for the business "Katina Graham LLC" was submitted. The application was signed and completed three days later on June 26, 2020.

22. The application includes all of GRAHAM's personal identifiers, including her name, date of birth, social security number, address, and phone number.

23. Internet service provider (ISP) records show that this EIDL application was submitted from an IP address that had been assigned to GRAHAM at the time of the application. The user name that GRAHAM had registered with her ISP is "thekatinagraham@gmail.com."

24. The application describes the business as a Maid and Cleaning Service with five employees that has been in business since February 7, 2016. Gross revenues were stated as \$117,897, cost of goods sold in the last 12 months were stated as \$27,654, and rental losses due to the disaster were stated as \$9,876.

25. According to the North Carolina Secretary of State business registration records, there was no registered business with the name “Katina Graham LLC” at the time of the EIDL application. GRAHAM registered four business with the North Carolina Secretary of State between 2008 and 2020. However, none of those businesses were active on June 23, 2020, when the EIDL application was submitted, or on January 31, 2020, when a business must have been in operation to be eligible for an EIDL loan. Katina Graham LLC would therefore be ineligible to receive the EIDL loan.

26. The primary contact e-mail for this loan application was “katinageneva@gmail.com” (i.e., SUBJECT ACCOUNT).

27. The affiant knows from experience that the EIDL loan process is conducted online, and the primary contact point for the loan applicant is the “Primary Contact” e-mail address, which is entered as part of the initial application. E-mails are sent from the SBA to this address in order to inform them of the loan process and any further steps that need to be taken by the applicant. Additionally, the final signature required by the applicant to complete the loan is completed online through the “DocuSign” service. Applicants receive an e-mail at their “Primary Contact” e-mail address where they are prompted to review the loan terms and then e-sign under the penalties of perjury that they have read and agree to such terms. Thus in this case, GRAHAM would have received the loan documents and terms at the SUBJECT ACCOUNT.

28. Based on the business and revenue information provided by GRAHAM in the application, the SBA approved an EIDL of \$40,100. The loan agreement was electronically signed by GRAHAM on June 26, 2020. The terms of the EIDL expressly state that the funds must be used by the business solely as working capital to alleviate economic injury caused by disaster.

29. On June 30, 2020, \$40,100 in EIDL funds were deposited into a bank account in GRAHAM's name at the Carolinas Telco Federal Credit Unit ("CTFCU"). On July 7, 2020, an advance of \$5,000 associated with the loan was deposited into the same account.

30. Bank records and other supporting documentation were received from CTFCU during the course of the investigation. Those records reveal that GRAHAM opened this account on January 10, 2020. GRAHAM's correct name, date of birth, address, SSN, and driver's license number are listed on the application. The contact e-mail listed is "katinageneva@gmail.com" (i.e., SUBJECT ACCOUNT).

31. Bank records show that following the EIDL deposits, large amounts of money were moved out of the account in various forms. Between June 30, 2020, and July 28, 2020, a total of \$6,450 was withdrawn in cash, and \$21,718.55 in payments were made through the CashApp, Venmo, and Square mobile payment services. Based on records received from the CashApp service, \$14,746.55 of this appears to be payments that GRAHAM made to herself on CashApp. Additionally, a \$4,600 check to an apartment complex, with no apparent business purpose, was written on July 3, 2020. Further research into records received from CTFCU did not appear to show any apparent business activity in the account.

32. In an interview on April 26, 2021, GRAHAM admitted that she had been recruited to apply for EIDL loans for two of her businesses, but claimed that others had completed the actual applications for her, using personal and business information which she provided. She also admitted to owning and controlling the bank accounts where the funds from these loans had been deposited.

33. Based on this information, it appears that GRAHAM used the Google account "katinageneva@gmail.com" in furtherance of this scheme, and it is believed that these accounts

may contain evidence of her involvement, as well as communications that may implicate others in the scheme.

BACKGROUND CONCERNING GOOGLE¹

34. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

35. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

36. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google

¹ . The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lens.google.com; product pages on support.google.com; or product pages on about.google.com.

devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

37. Signing up for a Google Account automatically generates an email address at the domain “gmail.com”, like the e-mail accounts listed in Attachment A. That email address will be the log-in username for access to the Google Account. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

38. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Google.

39. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google’s website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol (“IP”) addresses used to register the account and accept Google’s terms of service, as well as the

IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

40. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

41. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

42. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. In addition, emails and attachments can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

43. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).


44. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation.

CONCLUSION

45. Based on the forgoing, I request that the Court issue the proposed search warrant.

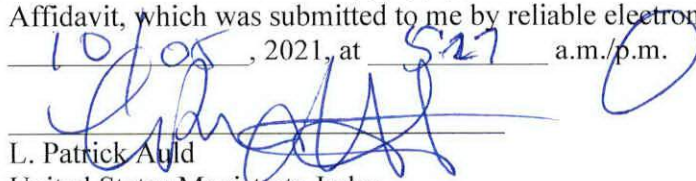
46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,


Steven S. Robinson
Special Agent
United States Secret Service

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this day of

10/05, 2021, at 5:27 a.m./p.m.


L. Patrick Auld
United States Magistrate Judge
Middle District of North Carolina